PÓSERNÉ OLÁH VALÉRIA

SZÁMÍTÓGÉP-HÁLÓZATI TÁMADÁSOK

BEVEZETÉS

Mára az otthonok nagy részében ugyanúgy megtalálható az Internet, mint a kormányhivatalokban, vagy épp az üzleti életben. Az Internetre kapcsolódó szerverek mindegyike számos adatbázist tartalmaz, vagy különböző, valamilyen egyéb szolgáltatást nyújt. **A felhasználók és a kiszolgálók száma napról napra növekszik, csakúgy, mint a szolgáltatások sokrétűsége**.

Az elmúlt években számtalan, világsajtót "rengető" hacker-akcióról hallhattunk, melyek többsége az Egyesült Államok ellen irányult. A New York-i Citybanktól elektronikus úton ellopott 10 millió dollár csak a jéghegy csúcsa volt. Az USA Hadügyminisztériumának rendszerében tárolt Desert Storm nevű hadművelet csapattelepítési dokumentumai ugyanúgy illegális letöltésre kerültek, mint a Dél-Koreai Atomfejlesztési Intézet titkos dokumentumai. Miután kiderült, hogy az akcióért egy 16 éves angol fiatal a felelős, el kellett fogadni azt a tényt, hogy nem lehetnek olyan titkok, amiket egy kellőképpen eltökélt hacker ne tudna megszerezni.

Naponta több száz sikeres, regisztrált feltörés történik a világhálón. Ebből **két - három naponta egy nagyobb rendszer** esik áldozatul valamilyen hacker-támadásnak. Az Amerikai Védelmi Minisztérium évente 200-300 ezer sikertelen feltörést ismer el, de, vajon mennyi azoknak a feltöréseknek a száma, amiket nem tár a nyilvánosság elé?

Az eddigiekből is látszik, hogy foglalkozni kell a témával annak jelentősége miatt, hiszen **a hálózati szolgáltatások, annak igénybevétele, az igénybevevők köre napról-napra nagyütemben bővül és szélesedik**, amiből eredően az élet egyre nagyobb területe válik sebezhetővé számítógép-hálózati támadások kapcsán.

A TÁMADÁSOK REGISZTRÁLÁSA

A felmérések szerint pl. **2004-ben összesen 392545 hackelést regisztráltak**, de a valós szám ennél lényegesen nagyobb. **A legnépszerűbb támadási forma az úgynevezett defacement**, azaz a weboldalak nyitóoldalának átalakítása általában úgy, hogy, hogy azonosítható legyen a támadó hacker vagy hacker-csoport.

A támadások motivációi:

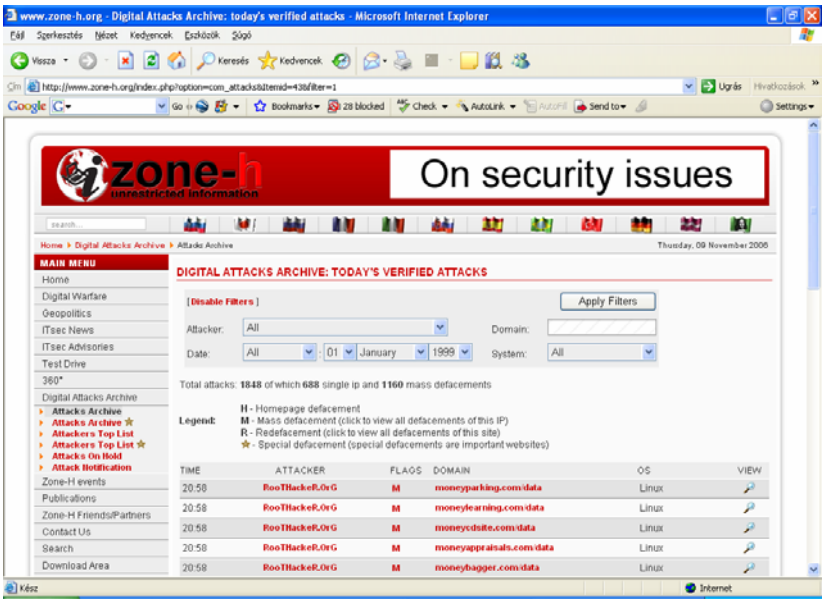
- Információ megszerzése (személyes, üzleti, katonai, stb.) haszonszerzés vagy károkozás céljából,
- szolgáltatásokhoz való illetéktelen hozzáférés (pl. nyomtatni, filmeket letölteni),
- szolgáltatások megbénítása,
- rendszer feltörése,
- rosszindulatú program(ok) bejuttatása,
- szórakozás, versengés pl. egy weboldal feltöréséért,
- politikai okokból,
- kifejezetten bűnös céllal (szerencsére csak kevés).

A támadásokért a weboldalak üzemeltetői is gyakran felelősek, mivel a támadások 55 százaléka olyan biztonsági réseken keresztül történik, amelyek ismertek a szakemberek előtt.

A hackelések száma különböző politikailag érzékeny évfordulókon észrevehetően megszaporodik, különösen az Egyesült Államok és az iszlám terroristák közötti konfliktusok évfordulóin. Egy vizsgálat azt is kimutatta, hogy a hosszabb munkaszüneti időszakok, például karácsony környéke is megemelik a támadások számát. [1]

A zone-h.org honlapról

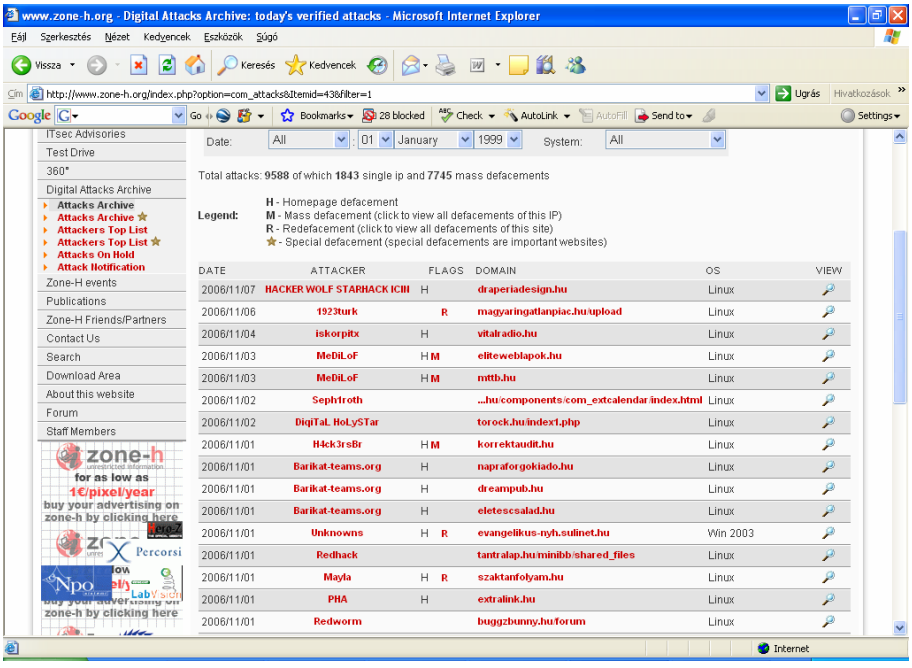
Drasztikus mértékben nő a weboldal-feltörések száma. A zone-h.org honlap (1. ábra) **szerverek biztonságáról**, illetve **sebezhetőségéről vezet listát**, és szinte percenként újabb és újabb feltört oldalról számol be. Az oldal listáihoz az adatokat többnyire maguk a támadók szolgáltatják, de bárkinek lehetősége van hírt adni egy-egy támadásról, és annak körülményeiről.



1. ábra: A zone-h.org oldala

Az oldal lehetőséget biztosít **támadások archívumból történő, támadóra, dátumra, domainre, valamint operációs rendszerre vonatkozó szűrt listájának megjelenítésére**. Külön menüpontból érhető el a kitüntetett szerepű, pl. kormányzati szerverek elleni támadások archívuma.

November első hetének statisztikáját szemlélve csak a magyar .hu domain-re vonatkozva 16 feltört honlapról ad hírt, és ez a szám még nem végleges. A listán neves, ismert és gyakran látogatott honlapok is szerepelnek (2. ábra).



2. ábra: A magyar domainek elleni támadások listája

Találomra kiválasztottam november első hetét és megvizsgáltam a támadások alakulását a leggyakoribb (Windows, Unix, Novell, Linux) operációs rendszerek esetében, idén, 2005-ben és 2004-ben ugyanebben az időszakban. Az eredményt az 1. 2. 3. táblázat, valamint az 1. sz. diagram szemlélteti.

	2004						
OS	**11. 1.**	**11. 2.**	**11. 3.**	**11. 4.**	**11. 5.**	**11. 6.**	**11. 7.**
Win 2003	3	24	13	18	22	23	55
Win XP	1	0	0	1	0	0	0
Win 2000	167	444	310	76	256	99	147
Win NT9X	12	109	52	9	25	176	13
Unix	0	0	0	0	0	0	0
NovellNetware	1	0	0	0	0	0	0
Linux	432	746	274	109	323	221	659
Egyéb	97	325	54	43	36	36	34
Összesen:	713	1648	703	256	662	555	908

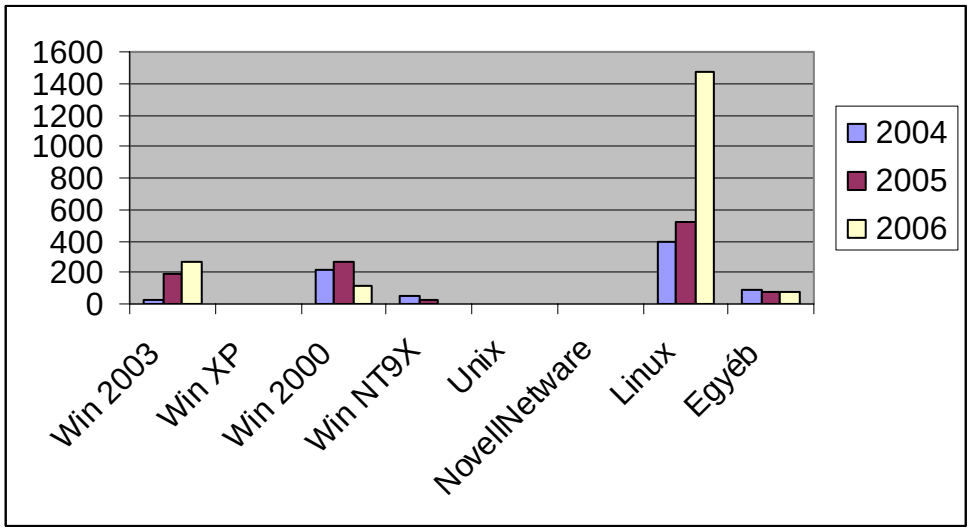
1. sz. táblázat: Támadások operációs rendszerenként 2004. nov. 1-7.

	2005						
OS	**11. 1.**	**11. 2.**	**11. 3.**	**11. 4.**	**11. 5.**	**11. 6.**	**11. 7.**
Win 2003	408	121	94	138	211	162	207
Win XP	2	2	2	0	2	1	1
Win 2000	264	251	131	113	437	337	321
Win NT9X	10	13	11	134	4	6	43
Unix	0	0	0	0	0	0	0
NovellNetware	0	0	0	0	0	0	0
Linux	307	493	707	249	793	715	365
Egyéb	56	92	105	34	65	103	62
Összesen:	1047	972	1050	668	1512	1324	999

2. sz. táblázat: Támadások operációs rendszerenként 2005. nov. 1-7.

	2006						
OS	**11. 1.**	**11. 2.**	**11. 3.**	**11. 4.**	**11. 5.**	**11. 6.**	**11. 7.**
Win 2003	393	143	222	157	252	471	228
Win XP	0	1	1	0	1	5	1
Win 2000	210	104	96	49	132	147	67
Win NT9X	15	1	2	0	3	2	5
Unix	1	0	0	0	0	1	0
NovellNetware	1	0	0	0	0	0	0
Linux	1550	769	1367	2124	2250	1077	1199
Egyéb	131	14	60	67	70	124	90
Összesen:	2301	1032	1748	2397	2708	1827	1590

3. sz. táblázat: Támadások operációs rendszerenként 2006. nov. 1-7.



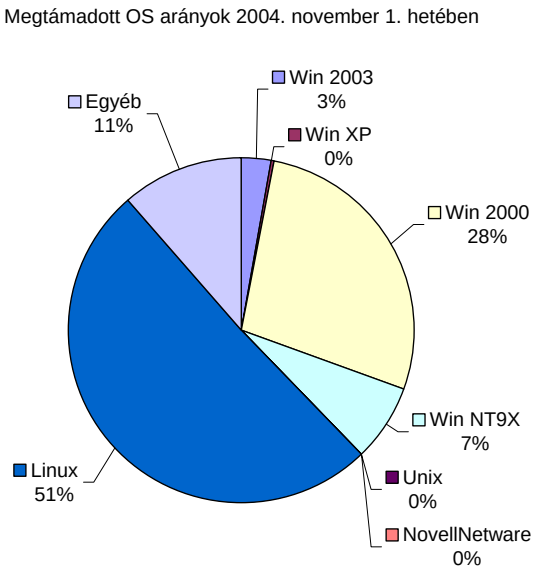
1. sz. diagram: Támadások operációs rendszerenként

Megállapítások:

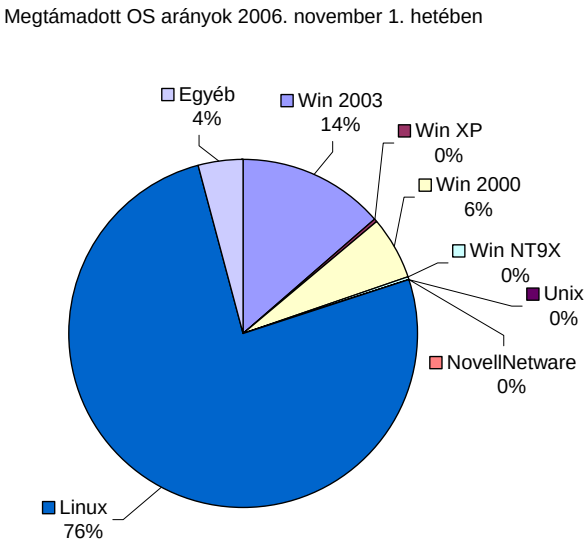
- A Windows operációs rendszerek esetében ugrásszerű változás nem tapasztalható. A **Windows 2003 támadásainak száma kismértékben növekszik**, ami betudható az operációs rendszer egyre szélesebb körű elterjedésének, **míg a Windows 2000, NT és 9X változatok** fokozatosan kiszorulnak a piacról, így érthető a **támadásuk számának kismértékű csökkenése**.
- Windows XP, Unix illetve NovellNetware rendszerek ellen a vizsgált időszakban csak 1-2 támadás történt, mely elhanyagolható.
- A **Linux rendszerek elleni támadások száma lényegesen magasabb, mint a Windows rendszereké**, ami érthető is, hiszen a legnépszerűbb támadási forma webszerverek ellen irányul, és köztudott, hogy webszervereket leginkább Linux rendszerek alatt üzemeltetnek. **A támadások száma azonban drasztikusan megnőtt**, ami elgondolkodtató, aggodalomra ad okot, és egyértelműen felhívja a figyelmet a Linux operációs rendszerek nagymértékű sebezhetőségére. Úgy vélem, hogy ennek oka a Linux verziók nagy számának, és részben a nyílt forráskódnak is köszönhető, hiszen számtalan változat biztonsági kérdéseit sokkal nehezebb karbantartani, mint pl. a néhány Windows változat biztonsági réseinek befoltozására koncentrálni.
- Már 2004-ben érzékelhető volt, hogy míg egy évvel korábban Linux és Windows rendszereket nagyjából azonos arányban törtek fel, 2004-ben a Linux már egyértelműen átvette a vezetést, átlagosan több, mint kétszer annyi esetben esett a nyílt forrású rendszerrel üzemelő kiszolgáló támadás áldozatául, mint a Microsoft

szoftverét futtató szerverek. [2]

- A **Windows és Linux rendszerek támadási különbségi aránya 2006-ra csak tovább nőtt**, melyet a 2. sz. és 3. sz. diagram jól mutat.



2. sz. diagram



3.sz. diagram

A LEGGYENGÉBB LÁNCSZEM AZ EMBER

Az előzőekben bemutattam, hogyan oszlik meg a támadások aránya a különböző alkalmazott operációs rendszerek esetében, most pedig ismertetnék egy szimulációs példát annak szemléltetésére, hogy **hiába választjuk ki legkörültekintőbben a megfelelő operációs rendszert, hiába alkalmazzuk a legkorszerűbb védekezési formákat, biztonságunk akkor is labilissá válhat.**

Egyik hallgatóm évekkel ezelőtt azt a tesztelési feladatot kapta, hogy támadja meg valamilyen formában egy társa számítógépét és vegye át az irányítást felette. A feladat kivitelezéséhez a NetBus nevű kliens-szerver architektúrában működő programot használta fel, mely Windows alapú rendszerek távoli irányítását tette lehetővé. A kliens egy grafikus felülettel is ellátott kisalkalmazás, mely segítségével kapcsolódhatunk a célgépen futó szerverhez (ehhez csupán a szerver IP címére van szükség). Sikeres kapcsolódás után a kliensről parancsokat (billentyűzet-figyelés, billentyű-lenyomás küldés, képernyőmentés, programindítás, fájlátvitel, a számítógép újraindítása, leállítása, a cd-meghajtó tálcájának kinyitása-becsukása, ablakok címeinek átírása stb.) küldhetünk a szervernek, melyek a célgépen hajtódnak végre.

A legnagyobb fejtörést az okozta, hogy hogyan juttassa el ismerőse gépére a NetBus szerverét, ráadásul úgy, hogy az el is induljon. Mint utóbb kiderült ez nem is volt olyan nehéz feladat, a szerver exe fájljának bejuttatása céljából írt Delphi-ben egy egyszerű játékot, melynek lényege az volt, hogy mozgó figurákat kellett lelőni az egérrel. A kész játék mappájába bemásolta az átnevezett NetBus szervert, hogy első látásra úgy tűnjön, a játékhoz tartozik. Beállította, hogy a játék indulásakor a szerver átmásolódjon a Windows egyik rendszer-mappájába, átneveződjön egy olyan exe fájlra, melynek neve hasonlít a Windows rendszerfájljainak nevéhez, és ezután elinduljon. A játékot egy zip fájlba csomagolva küldte át ismerősének ICQ-n keresztül, mondva, hogy egy játékot küld neki, amit nemrég talált az Interneten.

A társa kicsomagolta a játékot, teljesen megbízva ismerősében ellenőrzés és gyanakvás nélkül el is indította azt, így a NetBus szerver elindult a gépén. A szükséges IP címet pedig az ICQ – peer-to-peer chat program lévén ismeri a beszélgetőpartnerek IP címeit – Tools program (amely képes megjeleníteni a beszélgetőpartnerek IP címeit) segítségével szerezte meg. A játék iránt érdeklődve, közben folyamatosan chatelt ismerősével, aki folyamatosan beszámolt arról, hogy mindenféle értelmetlenséget művel a számítógépe.

A sikeres támadás után a nyomok eltüntetése céljából megszűntette a szerver automatikus indítását, beállította, hogy a Windows következő indításakor törlődjön az exe-fájl, és leállította a szerver éppen futó példányát.

Ez egy tipikus szimulálása volt annak az állításnak, hogy a leggyengébb láncszem az ember. Az ilyen támadások megelőzése érdekében gyanúval kell fogadni minden kívülről érkező fájlt is, még akkor is, ha ismerőstől származik.

A NetBus lassan 10 éves, és sokáig igen népszerű támadóeszköz volt, ma már szinte mindegyik vírusirtó, illetve tűzfal detektálja, és automatikusan törli a NetBus klienseket és szervereket.

A példa ugyan néhány évvel ezelőtti, de aktualitását nem vesztette el. Felmérést végeztem hallgatóim körében, és az eredmény még ma is siralmas. 83 százalékuk ma is mindenféle fenntartás nélkül elfogadta volna a küldött zip fájlt és ellenőrzés nélkül futtatná az ismerőstől származó játékot. Ez a példa úgy gondolom jól alátámasztja minden számítógép felhasználó – nem csak az informatikai szakembereké – biztonsági területen történő képzésének, továbbképzésének elengedhetetlen szükségességét.

ÖSSZEGZETT KÖVETKEZTETÉSEK

A 21. században az egyes országok informatikai struktúrájának rohamos fejlődésének szükséges velejárója, hogy **az informatikailag fejlettebb országok egyre nagyobb veszélynek vannak kitéve**, hiszen a számítástechnika és az Internet a világgazdaság civilszférájától egészen a kormányzatokig mára csaknem mindenhol jelen van. Célpontnak számíthatnak a bankok, a közlekedés, a pénzügyi rendszerek, a távközlés, a rendőrség, a katonai létesítmények, az energiaellátás, melyek esetleges támadása során az állami infrastruktúra is érzékenyen károsodhat, de célpont lehet akár az otthoni személyi számítógépünk is. **Egyedi gépeket támadhatnak pusztán szórakozásból, de azzal a céllal is, hogy a későbbiekben felhasználják azt egy komolyabb rendszer ellen indított támadás során**. Sokan úgy gondolkodnak, hogy, ha betörnek a gépükbe semmi gond, amíg az nem zavarja látványosan munkájukat, hiszen úgysincs semmi rejtegetni valójuk. Nincs a gépükön semmi fontos dolog, amit különösebben védeni kellene, és nem számolnak azzal a lehetőséggel, hogy számítógépük kapacitását felhasználhatják pl. egy fontos rendszer feltöréséhez.

Az élet szinte minden területét átszövik a számítógépes-hálózati rendszerek, így nem kis felelősség azok használata üzemeltetése. Nagyon gondosan kell a biztonságos üzemeltetés érdekében megtervezni, felépíteni és működtetni, de még felhasználni is egy ilyen rendszert, még akkor is, ha csak az otthoni, jelentéktelennek tűnő, Internetre kapcsolódó számítógépünkről van is szó.

Sokan hitet tettek a **nyílt forráskódú rendszerek** biztonságossága mellett, azonban annak vitathatatlan előnyei mellett óriási hátrányai is kezdenek kibontakozni. Ennek legfőbb okát a **számtalan verzió** létezésében látom, és mivel a Microsoft termékek esetén nem kell annyi változatra koncentrálni, így azok biztonsági kérdéseire több figyelmet tudnak szentelni. Ez tükröződik a támadási kísérletek vizsgálata során is, egyre inkább hátrányba kerül a Linux a Windows rendszerekkel szemben a biztonság területén.

Annak ellenére, hogy gondosan megválasztjuk a biztonságos működésnek legjobban megfelelő operációs rendszerünket **a legtöbb veszélyforrást együtt kapjuk a megvásárolt alkalmazásokkal,** nem tekinthetjük teljes mértékben a gyártókat felelősnek. Szükség van arra, hogy a felhasználók mindig körültekintően járjanak el. A biztonságtechnikai szakértők szerint a felhasználók figyelmetlensége egyre jobban nő, sőt az is probléma, hogy sok ember könnyen csalás áldozatává válik. Egyre több jelszó, és pénzügyi adat válik elérhetővé

illetéktelenek számára. [3]

Fontos, hogy a felhasználó tisztában legyen a biztonsági kérdések fajsúlyával, és azok fontosságával. A legtöbb esetben erre azonban csak minimális erőforrásokat koncentrálnak, nem számolnak azzal, hogy a tudatlan felhasználó, alkalmazott nagyságrendekkel nagyobb kárt is okozhat, mint amennyi hasznot hoz.

Különös gondot kell fordítani információs társadalmunk polgárainak az informatikai biztonság területén való megfelelő oktatására, hisz nem csak az informatikai szakembereknek van szüksége ezekre az ismeretekre, hanem a laikus felhasználóknak is, közös informatikai biztonságunk megteremtése érdekében.

FELHASZNÁLT IRODALOM

[1] Felmérték, hogy miért hackelnek a hackerek http://www.hvg.hu/Tudomany/20050425hacker.aspx 2005.04.25.

[2] Drasztikus mértékben nő weboldal-feltörések száma http://pcforum.hu/hirek/9581/Drasztikus+mertekben+no+weboldal-feltoresek+szama.html 2005.05.05.

[3] Még több támadás érheti majd a windowsos rendszereket 2004-ben http://www.sg.hu/cikkek/30296/meg_tobb_tamadas_erheti_majd_a_windowsos_rendszereket_2004_ben 2006. 10.12.